Claims

1. A security system for repelling viruses in computers and computer networks, which security system is adapted to forward messages, characterized in that the security system includes a first sub-system (1) to detect unknown viruses, which sub-system (1) is adapted in connection with the forwarding of messages or with other action or, in a timed manner, to perform at least one action to activate unknown viruses.

2. A security system in accordance with Patent Claim 1, characterized in that it is adapted to forward an alarm caused by the detection of a virus to at least one system connected to the security system (2, 3).

3. A security system in accordance with Patent Claims 1 or 2, characterized in that it is adapted to break the connection to at least one other system (2, 3, 114) on the basis of an alarm caused by the detection of a virus.

4. A security system in accordance with any of Patent Claims 1-3, characterized in that it additionally includes a second sub-system (2) for forwarding messages from the first sub-system (1) to at least one system (3, 210, 114) connected to the security system.

5. A security system in accordance with any of Patent Claims 1-4, characterized in that it additionally includes a third sub-system (3) that is adapted to break the connection to at least one other sub-system (1, 2) upon receiving an alarm.

6. A security system in accordance with Patent Claim 5, characterized in that the second sub-system (2) includes an identifier which corresponds identifier of the apparatus (3) of the third sub-system.

7. A security system in accordance with any of Patent Claims 1-6, characterized in that the first sub-system (1) is adapted to monitor its actions to detect viruses.

8. A security system in accordance with Patent Claim 2, characterized in that the alarm is a message or at least a part of a message that is forwarded to the recipient quicker than other communications.

9. A security system in accordance with Patent Claim 5, characterized in that the third sub-system (3) includes at least one computer or one network element including a computer.

10. A security system in accordance with Patent Claim 2 or 8, characterized in that the alarm is forwarded via a separate connection.

11. A security system in accordance with Patent Claim 1, characterized in that the said action is one the following: altering the time data, altering the contents of the memory, handling of files or at least its partial simulation.

12. A security system in accordance with any of Patent Claims 1-11, characterized in that it is adapted to detect an activated virus when at least one of the following conditions is met: a change takes place in the first sub-system (1) prior to actions causing changes carried out by the first-mentioned sub-system, a change takes place in the first sub-system (1) that is not an action taken by the said sub-system to detect a virus, a message leaves for another system without command from the first sub-system (1), a message leaves for another system to a wrong address or to a system which no communication has been directed to, a message does not leave for another system although it has been sent there.

13. A security system in accordance with Patent Claim 1 or 11, characterized in that it is adapted to combine activation measures of viruses to take place either simultaneously or consecutively in time.

14. A security system in accordance with Patent Claim 1 or 11, characterized in that it is adapted to choose one or more of the following logics when trying to activate viruses: one defined by the user, pre-programmed or at least partially random logic.

15. A security system in accordance with Patent Claim 5, characterized in that to it has been connected parallel with a third sub-system (3) a system that is adapted to save a message sent from the third sub-system (3).

16. A security system in accordance with Patent Claim 15, characterized in that the first sub-system (1) is adapted to compare in a parallel system a message sent from the third sub-system (3) to the first sub-system (1) and additionally saved in the parallel system in order to detect an anomaly caused by a virus.

17. A security system in accordance with Patent Claim 15, characterized in that the above-mentioned parallel system is adapted to forward a message saved by it.

18. A security system in accordance with any of Patent Claims 1-17, characterized in that it is adapted to examine messages forwarded though it in order to detect known viruses.

19. A security system in accordance with Patent Claim 4, characterized in that in order to isolate data between the first (114) and the second (3) system, it has been adapted to transfer data between the first (114) and the second (3) system through the first (1) and the second (2) sub-system, which security system is adapted to disrupt the connection between the first system (114) and the first (1) sub-system before a connection is established between the first (1) and the second (2) sub-system, and is adapted to disrupt the connection between the first (1) and the second (2) sub-system before a connection is established between the second sub-system (2) and the second system (3).

20. A security system for repelling viruses in computers and computer networks, which security system is adapted to forward messages, characterized in that the security system includes a first sub-system (1) for detecting unknown viruses, which first sub-system (1) is adapted to compare messages with at least partially identical identifiers with each other in order to detect unknown viruses.

21. A security system in accordance with Patent Claim 20, characterized in that it is adapted to request the sender of the above-mentioned messages with the same identifiers to re-send at least one message with the same identifier and further adapted to compare at least one re-sent message received with the above-mentioned original messages in order to detect messages containing viruses.

22. A method for repelling viruses in computers and data networks, characterized in that it is carried out in a security system including a first sub-system (1) for forwarding messages and for detecting viruses, which first sub-system (1) can, with regard to data transfer, be isolated from the rest of the system, which method includes the steps where:
- the functions of the system are monitored in order to detect a virus (311),

- a virus (312) is detected when at least one of the following conditions are met: a change takes place in the first sub-system (1) prior to actions causing changes carried out by the first-mentioned sub-system, a change takes place in the first sub-system (1) that is not an action taken by the said sub-system to detect a virus, a message leaves for another system without command from the first sub-system (1), a message leaves for another system to a wrong address or to a system which no communication has been directed to, a message does not leave for another system although it has been sent there,
- an alarm (316) is given.

23. A method for repelling viruses in computers and computer networks, characterized in that the method has stages where:
- at least one action in the system is taken in connection with the forwarding of messages or other action, or in a timed manner, in order to activate a virus (310),
- the actions of the system are monitored in order to detect an occurrence initiated by virus activation (311),
- an alarm (316) is given when a virus is detected (312).

24. A method in accordance with Patent Claim 23, characterized in that the system running it includes a first sub-system (1) for forwarding of messages and for detecting of viruses, which first sub-system (1) can be isolated from another system as to communications.

25. A method in accordance with Patent Claim 23, characterized in that the action taken to activate a virus is one of the following: altering the time data, altering the contents of the memory, handling of files or at least its partial simulation.

26. A method in accordance with Patent Claim 23, characterized in that it is run in a security system including a first sub-system (1) and a second sub-system (2) in which method the activation of a virus is detected when at least one of the following conditions is met: a change takes place in the first sub-system (1) prior to actions causing changes carried out by the first-mentioned sub-system, a change takes place in the first sub-system (1) that is not an action taken by the said sub-system to detect a virus, a message leaves for another system without command from the first sub-system (1), a message leaves for another system to a wrong address or to a system which no

communication has been directed to, a message does not leave for another system although it has been sent there.

27. A method in accordance with Patent Claim 23, characterized in that in order to activate a virus, activation measures are combined to take place either simultaneously or consecutively in time.

28. A method in accordance with Patent Claim 23, characterized in that the logic to be used when trying to activate a virus is one of the following: one defined by the user, pre-programmed or at least partially random logic.

29. A method in accordance with Patent Claim 23, characterized in that it also includes a stage where known viruses (306) are searched for on the basis of their characteristics.

30. A method in accordance with Patent Claim 23, characterized in that in order to isolate data between the first (114) and the second (3) system the method is run in a security system that includes a first (1) and a second (2) sub-system through which sub-systems (1, 2) data is transferred between the first (114) and the second (3) system phase by phase, in which phases:

- the connection for data transfer is disrupted between the first system (114) and the first sub-system (1),
- a connection for data transfer is established between the first sub-system (1) and the second sub-system (2),
- the connection for data transfer is disrupted between the first sub-system (1) and the second sub-system (2),
- a connection for data transfer is established between the second sub-system (2) and the second system (3).

31. An apparatus for repelling viruses in computers and computer networks, which apparatus includes equipment for saving data (610, 612) and for handling data (614) and equipment for transferring data (608) with another apparatus, characterized in that the apparatus is adapted to receive a message from the said other apparatus and to perform at least one action to activate viruses contained in the message.

32. An apparatus in accordance with Patent Claim 31, characterized in that the action mentioned is at least one of the following: altering the time

data, altering the contents of the memory, handling of files or at least its partial simulation.

33. An apparatus in accordance with Patent Claims 31 or 32, characterized in that it is adapted to detect virus activation when at least one of the following conditions is met: a change takes place prior to actions caused by changes made by the apparatus, a change takes place that is not an action taken by the apparatus to detect a virus.

34. An apparatus in accordance with Patent Claims 31 or 32, characterized in that it is adapted to send a message to either a sub-assembly of the apparatus or to the other apparatus mentioned, and it is adapted to detect virus activation when at least one of the following conditions is met: a message leaves without authorization from the anti-virus software of the apparatus, a message leaves for an address it has not originally been directed to, a message does not leave although it has been given a command to be sent.

35. An apparatus in accordance with Patent Claim 31, characterized in that it is adapted to combine virus activation measures to take place either simultaneously or consecutively in time.

36. An apparatus in accordance with Patent Claim 31, characterized in that it is adapted to choose as the logic to be used when trying to activate a virus one of the following: one defined by the user, pre-programmed or at least partially random logic.

37. An apparatus in accordance with Patent Claim 31, characterized in that it is adapted to examine the message mentioned in order to detect known viruses.

38. An apparatus in accordance with Patent Claim 31, characterized in that it is adapted to monitor its functions in order to detect viru